IN THE CLAIMS

Please amend the claims as follows:

Claim 1 (Previously Presented): A method for storing and enabling access to data at a server, the method comprising:

receiving a hint at the server from a first device, the hint generated by executable code located on the first device;

receiving, at the server, data encrypted by using a key, the key generated by performing a hashing algorithm on the hint and a password; and

sending the hint to a second device.

Claim 2 (Original): The method of claim 1, wherein the step of performing a hashing algorithm includes hashing the password.

Claim 3 (Previously Presented): A method for storing and enabling access to data at a server, the method comprising:

receiving a hint at the server from a first device, the hint generated by executable code located on the first device; and

receiving, at the server, data encrypted by using a key, the key generated by performing a hashing algorithm on the hint and a password, wherein

performing the hashing algorithm includes hashing the password to derive a first secret, hashing the first secret to derive a second secret, hashing the hint and the first secret to generate an intermediate index, and hashing the intermediate index and the second secret to generate the key.

Claim 4 (Previously Presented): A system, comprising:

a user interface configured to obtain a password;

a key generator coupled to the user interface configured to perform a hashing algorithm on a hint and the password to generate a key;

an encryption engine coupled to the key generator configured to encrypt data stored on a device using the key;

a communications module coupled to the encryption engine configured to send the encrypted data and the hint to a server for storage.

Claim 5 (Previously Presented): The system of claim 4, further comprising:

a hint generator configured to generate the hint.

Claim 6 (Original): The system of claim 4, wherein the key generator hashes the password.

Claim 7 (Previously Presented): A system, comprising:

a user interface configured to obtain a password;

a key generator coupled to the user interface configured to perform a hashing algorithm on a hint and the password to generate a key wherein the key generator hashes the password to derive a first secret, hashes the first secret to derive a second secret, hashes the hint and the first secret to generate an intermediate index, and hashes the intermediate index and the second secret to generate the key;

an encryption engine coupled to the key generator configured to encrypt data stored on a device using the key; and

a communications module coupled to the engine configured to send the encrypted data to a server for storage.

Claim 8 (Currently Amended): A system, comprising:

means for obtaining a hint;

means for obtaining a password through [[and]] an interface to executable code transmitted to a device;

means for performing a hashing algorithm on the hint and the password to generate a key;

means for encrypting data stored on the device using the key; and

means for sending the encrypted data to a server for storage.

Claim 9 (Previously Presented): The system of claim 8, wherein the executable code is stored on a computer-readable storage medium.

Claim 10 (Previously Presented): The system of claim 8, wherein the system is configured to transmit the executable code embodied in a carrier wave.

Claim 11 (Previously Presented): A method for storing and enabling access to data at a server, the method comprising:

receiving, at the server, a request to store encrypted data from a device;

sending an encryption downloadable to the device for deriving a key to encrypt data stored at the device;

receiving, at the server, encrypted data encrypted by the encryption downloadable from the device;

receiving, from the device, a hint, corresponding to the encrypted data and used for regenerating the key; and

storing the hint and the encrypted data at the server.

Claim 12 (Currently Amended): A system, comprising:

an encryption downloadable configured to derive an encryption key from a password and a hint;

a web server configured to interface with a device and send the encryption downloadable to the device, and receive data encrypted by the encryption downloadable from the device; and

a memory coupled to the web server configured to store a hint corresponding to the encrypted data and used to regenerate the key from the ~~client~~ device and the encrypted data.

Claim 13 (Previously Presented): A method, comprising;

receiving, at a device, encrypted data and a hint corresponding to the encrypted data from a server; inputting a password through an interface to executable code; and

performing a hashing algorithm on the password and the hint at the device to generate a key for decrypting the encrypted data.

Claim 14 (Previously Presented): The method of claim 13, wherein performing the hashing algorithm further includes hashing the password.

Claim 15 (Previously Presented): A system, comprising:

a user interface configured to obtain a password;

a communication module configured to send encrypted data and a hint corresponding to the encrypted data from a server to a device; and

a key generator for performing a hashing algorithm on the password and the hint at the device to generate a key for decrypting the encrypted data.

Claim 16 (Previously Presented): A system, comprising:

means for obtaining a password through an interface to executable code transmitted to a device;

means for sending encrypted data and a hint corresponding to the encrypted data from a server to the device; and

means for performing a hashing algorithm on the password and the hint at the device to generate a key for decrypting the encrypted data.

Claim 17 (Previously Presented): The system of claim 16, wherein the executable code is stored on a computer-readable storage medium.

Claim 18 (Previously Presented): The system of claim 16, wherein the system is configured to transmit the executable code embodied in a carrier wave.

Claim 19 (Previously Presented): A method, comprising:

receiving information identifying encrypted data stored at a server;

sending a decryption downloadable to a device, the decryption downloadable deriving a key from a password and a hint;

sending the hint corresponding to the encrypted data to the device; and

deriving the key by hashing at least one of the hint and the password.

Claim 20 (Currently Amended): A system, comprising:

a decryption downloadable configured to derive a key by hashing at least one of a password and a hint corresponding to encrypted data;

a memory configured to store the encrypted data and [[a]] the hint corresponding to the encrypted data; and

a web server configured to interface with the device, and send the decryption downloadable, the encrypted data, and the hint to the client.

Claim 21 (Previously Presented): A device based method, comprising:

obtaining a password through an interface to executable code transmitted to the device;

deriving a first secret from the password;

receiving a hint corresponding to data to be decrypted from a server;

deriving an intermediate index from the first secret and the hint; and

sending the intermediate index to the server, the intermediate index used to decrypt data stored on the server.

Claim 22 (Previously Presented): The method of claim 21, wherein deriving the first secret further includes hashing the password.

Claim 23 (Previously Presented): The method of claim 21, wherein deriving an intermediate index further includes hashing the first secret and the hint.

Claim 24 (Previously Presented): A system, comprising:

a user interface configured to obtain a password;

an index generator coupled to the user interface configured to generate an intermediate index from a hint received from a server and a secret derived from the password; and

a communications engine coupled to the index generator configured to send the intermediate index to the server.

Claim 25 (Previously Presented): The system of claim 24, wherein the index generator is further configured to generate the intermediate index by hashing the hint and the secret.

Claim 26 (Previously Presented): A system, comprising;

means for obtaining a password through an interface to executable code transmitted to a device;

means for deriving a first secret from the password;

means for receiving a hint corresponding to data to be decrypted from a server;

means for deriving an intermediate index from the first secret and the hint; and

means for sending the intermediate index to the server, the intermediate index used to decrypt data stored at the server.

Claim 27 (Currently Amended): The system of claim 26, wherein [[the]] the executable code is stored on a computer-readable storage medium.

Claim 28 (Previously Presented): The system of claim 26, wherein the system is configured to transmit the executable code embodied in a carrier wave.

Claim 29 (Previously Presented): A server-based method, comprising;

receiving from a device, a request for access to data stored at a server;

transmitting to the device a hint corresponding to the data, and a decryption downloadable for deriving an intermediate index from a password and the hint;

receiving the intermediate index from the device; and

deriving a decryption key from a second secret corresponding to the device and the intermediate index.

Claim 30 (Currently Amended): A system, comprising;

a memory configured to store a second secret corresponding to a device;

a decryption downloadable configured to generate an intermediate index from a password and a hint corresponding to encrypted data;

a web server configured to receive information identifying the encrypted data to be decrypted, transmit the decryption downloadable and [[a]] the hint corresponding to the ~~indication~~ encrypted data to the device, and receive an intermediate index from the device; and

a server-resident module configured to derive a key for decrypting the encrypted data from the second secret and the intermediate index.